

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

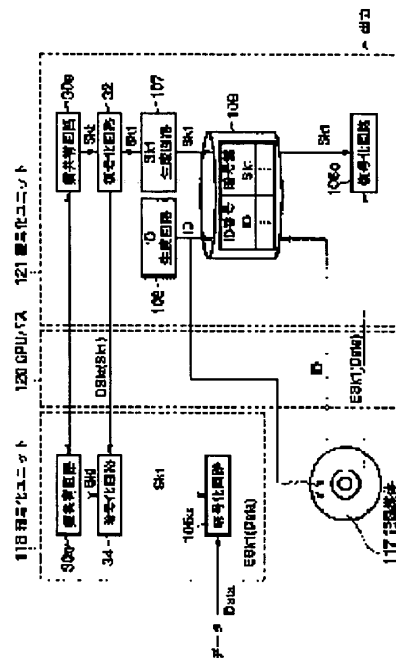
(11)Publication number : 10-293724
(43)Date of publication of application : 04.11.1998

G06F 12/14
G09C 1/00
H04L 9/08
H04L 9/10

(71)Applicant : TOSHIBA CORP
(72)Inventor : KATO TAKEHISA
ENDO NAOKI

(57)Abstract:

SOLUTION: This system is provided with a ciphering unit 118 and a decoding unit 121 and the ciphering unit 118 and the decoding unit 121 are connected to the CPU bus 120 of a personal computer. Then, at the time of ciphering one set of data, the data ciphering key Sk1 used for the ciphering of the data is generated, a pair with the identification information ID is generated, the pair is recorded in a database and the information of the ID and the data ciphered by the Sk1 are recorded in a recording medium 117. Then, at the time of reproduction, the data ciphering key Sk1 is obtained from the database based on the information of the ID read from the recording medium 117 and the ciphered data recorded in the recording medium 117 are decoded with the data ciphering key Sk1 as a decoding key.



[Date of request for examination]	11.09.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10293724 A**(43) Date of publication of application: **04 . 11 . 98**

(51) Int. Cl.

G06F 12/14
G09C 1/00
H04L 9/08
H04L 9/10

(21) Application number: **09102055**(71) Applicant: **TOSHIBA CORP**(22) Date of filing: **18 . 04 . 97**

(72) Inventor: **KATO TAKEHISA**
ENDO NAOKI

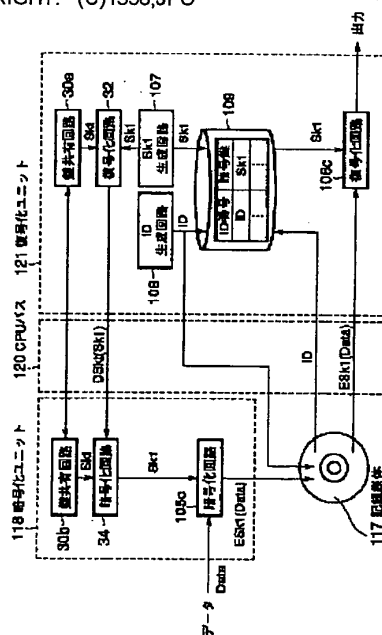
(54) **UNIT DEVICE, DECODING UNIT DEVICE,
 CIPHERING UNIT DEVICE, CIPHERING SYSTEM,
 CIPHERING METHOD AND DECODING METHOD**

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized copying by a third person by recording a data ciphering key generated every time inside a unit corresponding to identification information.

SOLUTION: This system is provided with a ciphering unit 118 and a decoding unit 121 and the ciphering unit 118 and the decoding unit 121 are connected to the CPU bus 120 of a personal computer. Then, at the time of ciphering one set of data, the data ciphering key Sk1 used for the ciphering of the data is generated, a pair with the identification information ID is generated, the pair is recorded in a database and the information of the ID and the data ciphered by the Sk1 are recorded in a recording medium 117. Then, at the time of reproduction, the data ciphering key Sk1 is obtained from the database based on the information of the ID read from the recording medium 117 and the ciphered data recorded in the recording medium 117 are decoded with the data ciphering key Sk1 as a decoding key.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-293724

(43) 公開日 平成10年(1998)11月4日

(51) Int. Cl.⁸

G 0 6 F

F 0 0

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 A

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

9/10

6 2 1 A

審査請求 未請求 請求項の数14 O L (全 26 頁)

(21) 出願番号 特願平9-102055
 (22) 出願日 平成9年(1997)4月18日

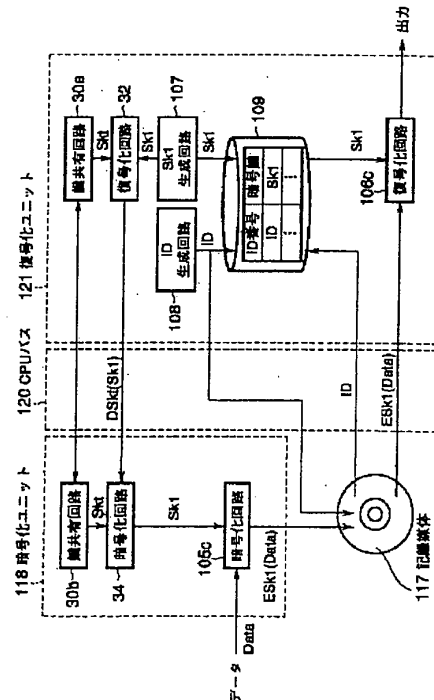
(71) 出願人 000003078
 株式会社東芝
 神奈川県川崎市幸区堀川町72番地
 (72) 発明者 加藤 岳久
 神奈川県川崎市幸区小向東芝町1番地 株
 式会社東芝研究開発センター内
 (72) 発明者 遠藤 直樹
 神奈川県川崎市幸区小向東芝町1番地 株
 式会社東芝研究開発センター内
 (74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 ユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法

(57) 【要約】

【課題】 第三者による不正コピーを防止可能な復号化装置を提供すること。

【解決手段】 記録媒体に記録された暗号化データを復号するCPUバスに接続される復号化装置であって、CPUバスを介さずに入力されたデータを暗号化する暗号化装置が対象とするデータの識別番号と該データのための暗号鍵を生成するための手段と、暗号鍵と識別番号を対応付けて記録するための手段と、CPUバスを介して暗号化装置に暗号鍵を外部から取得されことなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されている暗号鍵のうちから、識別情報とこれに対応する暗号鍵で暗号化されたデータが記録された記録媒体から読み出されCPUバスを介して与えられた識別情報に対応する暗号鍵を求め、該暗号鍵を復号鍵として記録媒体から読み出されCPUバスを介して与えられた暗号化データを復号するための手段とを備えたことを特徴とする。



【特許請求の範囲】

【請求項1】 計算機のCPUバスを介さずに入力したデータを所定の記録媒体に記録する前に暗号化する装置のために、データ暗号化鍵を生成し記録する、計算機のCPUバスに接続されて使用されるユニット装置であって、

暗号化対象となるデータの識別番号を生成するための手段と、

前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化する装置に前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に伝えるための手段とを備えたことを特徴とするユニット装置。

【請求項2】 暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、

前記計算機のCPUバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、

前記暗号化ユニット装置が前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化ユニット装置。

【請求項3】 暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、

前記計算機のCPUバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、

前記暗号化ユニット装置が前記データと前記識別情報の暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝えるための手段と、

自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、

10 求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化ユニット装置。

【請求項4】 前記データ暗号化鍵を求めるための手段は、自装置内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自装置内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自装置内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものであることを特徴とする請求項3に記載の復号化ユニット装置。

【請求項5】 前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さず外部に出力するための手段をさらに備えたことを特徴とする請求項2ないし4のいずれか1項に記載の復号化ユニット装置。

【請求項6】 暗号化ユニット装置

30 計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、

暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらに対応付けて記録する装置から、前記計算機のCPUバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする暗号化ユニット装置。

【請求項7】 暗号化ユニット装置

計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、

暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらに対応付けて記録し、与えられた識別情報またはデータ暗号化鍵で暗号化された識別情報をもとにして求めたデータ暗号化鍵を

用いて与えられた暗号化されたデータを復号する復号化ユニットから、前記計算機のCPUバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする暗号化ユニット装置。

【請求項8】 計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、

前記復号化ユニットは、

暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、

前記データの識別番号を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段を備え、

前記暗号化ユニットは、

前記計算機のCPUバスを介して前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする暗号処理システム。

【請求項9】 計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、

前記復号化ユニットは、

暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、

前記データの識別番号を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段を備え、

前記暗号化ユニットは、

前記計算機のCPUバスを介して前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータと受け取った前記識別情報とをそれぞれ暗号化するための手段とを備えたことを特徴とする暗号処理システム。

【請求項10】 前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、

前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、

前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えたことを特徴とする請求項8または9に記載の暗号処理システム。

【請求項11】 計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いて、該CPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、

前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、

前記復号化ユニットから前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝え、

前記暗号化ユニットにて、前記暗号化対象となるデータを伝えられた前記データ暗号化鍵で暗号化することを特徴とする暗号化方法。

【請求項12】 所定の記録媒体に識別情報とともに記録

された暗号化されたデータを、計算機のCPUバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、

自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求め、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号することを特徴とする復号化方法。

【請求項13】計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いて、該CPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、

前記復号化ユニットから前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝え、前記暗号化ユニットにて、前記暗号化対象となるデータと伝えられた前記識別情報とを、伝えられた前記データ暗号化鍵でそれぞれ暗号化することを特徴とする暗号化方法。

【請求項14】所定の記録媒体に暗号化された識別情報とともに記録された暗号化されたデータを、計算機のCPUバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、

自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記CPUバスを介して与えられたデータ暗号化鍵で暗号化された識別情報に対応するデータ暗号化鍵を求め、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号することを特徴とする復号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデータをネットワークを介して通信を行うシステムあるいは前記デジタルデータを記録保存し、読み出しするシステムのためのユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法に関する。

【0002】

【従来の技術】現在、計算機が広範に普及しており、種々の分野で情報を電子化して処理し、あるいは情報を電子化して記録装置に保存することが通常行われるようになってきている。また、ネットワーク環境も益々整ってきており、情報を電子化して送信することも通常行われるようになってきている。さらには、文書情報だけでなく、音声や画像などのデータを電子化して扱う技術も急速に進歩してきている。

【0003】ところで、電子化して扱う情報には、もちろん企業秘密や個人情報のように秘匿性を要する情報が含まれる。また、著作権に係る情報のように扱いに注意を要する情報も含まれる。

【0004】そこで、情報を電子化して扱う際に、暗号化を行っておき、正当な者だけがこれを復号できるようにする技術が良く使われている。例えば、データを暗号化して記録媒体に保存し、また記録媒体から暗号化データを読み出して復号し元のデータを取り出す暗号システムでは、予め暗号化と復号に用いる秘密鍵を定めておき、この秘密鍵を用いて保存、読み出しが行われる。このシステムによれば、秘密鍵を用いることができる者だけが保存された暗号化データを復号することができ、秘密鍵が解読されない限り、秘密鍵を用いることができない第三者が暗号化されたデータを不正に解読することはできない。

【0005】

【発明が解決しようとする課題】しかしながら、上記システムでは、もし第三者の不正な攻撃により秘密鍵が解読されると、すべての暗号化データが解読されるばかりでなく、解読により得たデータ（プレーンデータ）を自由にコピーすることが可能となってしまう。

【0006】また、秘密鍵が解読されなくても、他の暗号化システムにも同一の秘密鍵を内蔵するような場合には、暗号化データをそのままコピーすることにより、簡単に海賊版の作成ができてしまう。

【0007】さらに、秘密鍵が暴かれたことが発覚した場合、該当する暗号化システムの秘密鍵を更新する必要があるが複雑であるだけでなく、秘密鍵の更新後には当該暴かれた秘密鍵が復号にも使用できなくなるような更新形態をとるシステムにおいては、秘密鍵の更新後は当該暴かれた秘密鍵で暗号化されていたデータを復号することができなくなり、正当な者も元の内容を得ることができなくなってしまう不具合がある。

【0008】本発明は、上記事情を考慮してなされたものであり、第三者による不正なコピーを防止することができるユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【0009】また、本発明は、第三者が鍵情報を取得しあるいは暗号化データを解読することを困難にするユニ

ット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【0010】さらに、本発明は、鍵情報の更新手続きを不要とするユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は、計算機のCPUバスを介さずに入力したデータ（デジタル化されたデータ；例えば、文書、音声、画像、プログラムなど）を、所定の記録媒体に記録する前に暗号化する装置のために、データ暗号化鍵を生成し記録する、計算機のCPUバスに接続されて使用されるユニット装置であって、暗号化対象となるデータの識別番号を生成するための手段と、前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化する装置に前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されことなく安全に伝えるための手段とを備えたことを特徴とする。

【0012】本発明は、暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、前記計算機のCPUバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、前記暗号化ユニット装置が前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されことなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【0013】本発明は、暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、前記計算機のCPUバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、前記暗号化ユニット装置が前記データと前記識別情報の暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ

暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されことなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵と暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【0014】好ましくは、前記データ暗号化鍵を求めるための手段は、自装置内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自装置内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自装置内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものである。

【0015】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さずにより外部に出力するための手段をさらに備えても良い。

【0016】本発明は、計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらに対応付けて記録する装置から、前記計算機のCPUバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されことなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする。

【0017】本発明は、計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらに対応付けて記録し、与えられた識別情報またはデータ暗号化鍵で暗号化された識別情報をもとにして求めたデータ暗号化鍵を用いて与えられた暗号化されたデータを復号する復号化ユニットから、前記計算機のCPUバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されことなく安全に受け取るための手段と、受

け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする。

【0018】本発明は、計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、前記復号化ユニットは、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記データの識別番号を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段を備え、前記暗号化ユニットは、前記計算機のCPUバスを介して前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする。

【0019】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さずに外部に出力するための手段をさらに備えても良い。

【0020】本発明は、計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、前記復号化ユニットは、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記データの識別番号を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化され

たデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段を備え、前記暗号化ユニットは、前記計算機のCPUバスを介して前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータと受け取った前記識別情報とをそれぞれ暗号化するための手段とを備えたことを特徴とする。

【0021】好ましくは、前記データ暗号化鍵を求めるための手段は、自ユニット内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自ユニット内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自ユニット内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものである。

【0022】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さずに外部に出力するための手段をさらに備えても良い。

【0023】好ましくは、前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えても良い。

【0024】本発明は、計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いて、該CPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、前記復号化ユニットから前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝え、前記暗号化ユニットにて、前記暗号化対象となるデータを伝えられた前記データ暗号化鍵で暗号化することを特徴とする。

【0025】本発明は、所定の記録媒体に識別情報とともに記録された暗号化されたデータを、計算機のCPUバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するデータ暗号化鍵を求め、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号すること

【0026】本発明は、計算機のCPUバスに接続された暗号化ユニットと復号化ユニットを用いて、該CPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、前記復号化ユニットから前記計算機のCPUバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝え、前記暗号化ユニットにて、前記暗号化対象となるデータと伝えられた前記識別情報とを、伝えられた前記データ暗号化鍵でそれぞれ暗号化することを特徴とする。

【0027】本発明は、所定の記録媒体に暗号化された識別情報とともに記録された暗号化されたデータを、計算機のCPUバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記CPUバスを介して与えられたデータ暗号化鍵で暗号化された識別情報に対応するデータ暗号化鍵を求め、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号することを特徴とする。

【0028】本発明によれば、データを暗号化した暗号鍵をデータに付与した識別情報に対応して復号化ユニット内にデータベースとして記録しておくことにより、データを暗号化した計算機（あるいはデータの暗号化に用いた復号化ユニットそのものを組み込んだ計算機）でなければ復号を行うことができない。したがって、記録媒体の複製を作っても他の計算機では復号することができない。

【0029】また、本発明によれば、データを暗号化するためのデータ暗号化鍵を、例えば共有化した一時鍵あるいはマスター鍵の鍵束の中の何れかを用いて暗号化するなどして、復号化ユニットと暗号化ユニットとの間で

CPUバスを介して共有するため、CPUバスからこれらの情報を記録することは無意味である。

【0030】また、本発明によれば、データを暗号化するデータ暗号化鍵自体も、またデータ暗号化鍵を共有化するために用いる一時鍵も、毎回変わるため、第3者に暗号を解読することは極めて困難である。

【0031】したがって、本発明によれば、第3者による不正なコピーを防止することが可能となる。また、本発明によれば、鍵情報の更新手続きが不要となる。

【0032】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。本実施形態では、データを暗号化して記録媒体に記録し、また記録媒体から暗号化データを読み出し復号するシステムを例にとって説明する。

【0033】本実施形態では、暗号化の操作を $E_y(x)$ と表す。ここで、 x は暗号化の対象となるデータであり、 y は暗号化に用いる暗号鍵である。また、復号化の操作を $D_y(z)$ と表す。ここで、 z は復号化の対象となるデータであり、 y は復号化に用いる復号鍵である。

【0034】本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵を x としデータを y とすれば、

$E_x(D_x(y)) = y$
で表される。

【0035】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機（以下、PC）内に備えられたCPU（図示せず）のCPUバスに接続され、全体的な処理の流れの制御はプログラムで実現される。本実施形態では、データの入出力はCPUバス以外の例えばI/Oポート等を通じて行われるが、ディスクドライブ装置（図示せず）とユニットとの間、ユニットとユニットとの間でのデータ転送には、CPUバスが用いられる。従って、CPUバス上を流れるデータには、暗号化（あるいは暗号化に先だって行う復号化）を施している。

【0036】本実施形態は、概略的には、一纏まりのデータを暗号化する際に、データの暗号化に用いるデータ暗号化鍵 $Sk1$ と識別情報IDの対を生成し、この対をデータベースに記録しておくとともに、記録媒体にはIDの情報と $Sk1$ で暗号化したデータを記録し、再生時には記録媒体から読み出したIDの情報をもとにデータベースから $Sk1$ を求め、 $Sk1$ を復号鍵として記録媒体に記録された暗号化データを復号するものである。

【0037】第1, 3の実施形態ではIDを暗号化せず
に記録媒体に記録する例を、第2, 4の実施形態ではI
Dをデータ暗号化鍵で暗号化して記録する例を示す。第
1, 3の実施形態では、データを暗号化した暗号鍵の検
索を容易にし、復号時間を短縮することが可能となる。
第2, 4の実施形態ではIDを暗号化して記録媒体に記
録することにより、暗号化されたデータをより厳密に第
3者から守ることが可能となる。

【0038】また、第1, 2の実施形態ではCPUを介
したユニット間で鍵を共有する1つの例を、第3, 4の
実施形態ではCPUを介したユニット間で鍵を共有する
他の1つの例を示す。

【0039】(第1の実施形態) 図1は、本発明の第1
の実施形態に係るシステムの構成を示すブロック図であ
る。なお、図1の鍵共有回路30a, 30bの内部構成
の一例を図2に示す。また、図3に本システムの暗号化
の際の手順を、図4に鍵共有手順の一例を、図5に本シ
ステムの復号の際の手順をそれぞれ示す。

【0040】図1に示すように、本実施形態に係るシ
ステムは、暗号化ユニット118と復号化ユニット121
を備えている。また、暗号化ユニット118と復号化ユ
ニット121は、PCのCPUバス120に接続されて
いる。

【0041】また、CPUバス120にはディスクド
ライブ装置(図示せず)が接続されており、ディスクド
ライブ装置により記録媒体117への読み書きが行われ
る。図1に示すように、暗号化ユニット118は、鍵共
有回路30b、暗号化回路34, 105cを備えてい
る。暗号化ユニット118は、独立した1つのICチッ
プとして形成されるものとする。

【0042】復号化ユニット121は、データ暗号鍵生
成回路107、ID生成回路108、復号化回路32,
106c、ID/鍵情報記憶回路109を備えている。
復号化ユニット121は、独立した1つのICチップと
して形成されるものとする。

【0043】なお、全体の制御は図示しない制御部が司
るものとする。制御部は例えばプログラムを当該PCの
CPUで実行することにより実現することができる。デ
ータDataは、暗号化して記録する対象となる入力デ
ータであり、例えばPCのI/Oポートから入力される
映像、音声、テキストなどのマルチメディア・データで
ある。

【0044】IDは、本実施形態では、一纏まりのデー
タ毎(例えばタイトル毎)に与えられる識別番号であ
る。なお、IDは、ディスク毎に与えるようにしても良
いし、ディスクの片面毎あるいは複数のディスクからな
る組毎に与えるようにしても良いし、上記の一纏まりの
データをさらに細分化した部分毎(例えばチャプター毎
あるいは曲毎など)に与えるようにしても良い。

【0045】Sk1は、データの暗号化および復号に用

いるデータ暗号鍵(共通鍵暗号方式における共通鍵)で
あり、IDと対で生成される。Sk1は、CPUバス1
20上に情報を流す際に、該情報を復号(暗号化に先だ
って行う復号)するための、その都度変化する一時鍵
(共通鍵暗号方式における共通鍵)である。

【0046】ID生成回路108は、ID番号を生成す
る。ID番号は、1から順番に発番するようにしても良
いが、好ましくはランダムに発番する方が良い。後者の
場合、生成されるIDが全て異なるようにするために、
例えばID生成回路108を乱数発生器を用いて構成す
る方法が考えられる。なお、重複発番する可能性のある
乱数等を用いる場合には、生成したIDが既発番のもの
と同じであるかどうかチェックし、重複して発番された
ことが分かったならば、そのIDは破棄し、別のIDを
生成し直すようにすると好ましい。

【0047】データ暗号鍵生成回路107は、IDと対
になるデータ暗号鍵Sk1を生成する。データ暗号鍵生
成回路107は、例えば鍵長分の乱数発生器で構成して
も良い。また、乱数を発生するにあたって、例えば時計
(図示せず)からの時間情報を用いるようにしても良
い。なお、全てのビットが0や1になる可能性のある乱
数で鍵を生成する場合は、全てのビットが0や1になる
ことがないようにチェック処理等をする必要がある。

【0048】ID/鍵情報記憶回路109は、対になる
IDとSk1とを対応づけて記憶するためのものである。
例えば、IDとSk1をデータベース化して保管してお
く。鍵共有回路30a, 30bは、少なくとも論理的に
同一の構成を有し、後述する手順により相互に情報の受
け渡しをして同一の一時鍵(バス鍵)Sk1を生成し共
有する。復号化ユニット121と暗号化ユニット118
は、鍵共有回路30a, 30bを用いて、同一の一時鍵
Sk1を外部から知得されることなく安全に共有する。
鍵共有回路30a, 30bは外部からその内部の論理が
解析されないようにICチップ内に作り込むものとし
る。

【0049】記録媒体117は、暗号化されたI/Oポ
ートからの入力データを記録するためのものであり、例
えばハードディスク、MO、FD、1回書き込み可能な
CD、DVD-RAMなどを用いることが考えられる。

【0050】なお、ディスクドライブ装置内には、記録
の際に変調、誤り訂正回路を行い、再生の際に復調、誤
り訂正回路を行う変復調/誤り訂正回路が内蔵される場
合がある。

【0051】また、本実施形態では、復号化ユニット1
21にはデジタルデータDataをアナログデータに
変換するD/A変換回路が備えられ、復号化ユニット1
21からはアナログに変換されたデータが出力されるも
のとする。また、デジタルデータDataが復号すべ
きものである場合にはこれを復号する復号回路をD/A
変換回路の前に設けるものとする。例えばデジタルデ

ータDataがMPEG方式で圧縮された画像データである場合に、MPEG復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット121からの出力は例えば画像としてディスプレイなどに表示される。

【0052】最初に、図1～図4を参照しながら、暗号化の際の手順について説明する。なお、図4におけるCPUはプログラムで実現した場合の制御部に相当し、ここではCPUすなわち制御部が手順の仲介を行っていることを示している。なお、制御部の仲介なしにユニット間で直接情報のやり取りを行うようにしても構わない。

【0053】まず、記録媒体117がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。ステップS11では、復号化ユニット121にて、ID生成回路108により入力データに対するIDを生成する。また、データ暗号鍵生成回路107により入力データを暗号化するための暗号鍵Sk1を生成する。そして、生成されたIDとSk1とを対応付けて復号化ユニット121内の記憶領域109に記録しておく。また、生成されたIDを記録媒体117に記録する。

【0054】なお、IDは、復号化ユニット121からCPUバスを介して直接、ディスクドライブ装置に与えても良いし、復号化ユニット121からCPUバスを介して暗号化ユニット118に与え、暗号化ユニット118からCPUバスを介してディスクドライブ装置に与えるようにしても良い。

【0055】ステップS12では、復号化ユニット121と暗号化ユニット118との間で鍵共有手順により一時鍵Sk tを共有する。ここでは、「日経エレクトロニクス No. 676 pp. 13-14 1996. 1. 1. 18」に開示された技術を応用するものとする。

【0056】まず、本実施形態における鍵共有手順に用いる図2に示される鍵共有回路30a、30bの構成について説明する。鍵共有回路30aは、チャレンジ鍵生成回路31a、認証鍵生成回路33a、比較回路35a、バス鍵生成回路37aを備えている。また、鍵共有回路30bは、チャレンジ鍵生成回路31b、認証鍵生成回路33b、比較回路35b、バス鍵生成回路37bを備えている。

【0057】チャレンジ鍵生成回路31a、31bは、例えば乱数生成アルゴリズムを用いて、生成の都度変化するチャレンジ鍵を生成する。認証鍵生成回路33a、33bは、例えば一方性関数を用いて、チャレンジ鍵から認証鍵を生成する。

【0058】比較回路35a、35bは、2つの認証鍵が一致するか否かを比較する。バス鍵生成回路37a、37bは、例えば一方性関数を利用して、2つの認証鍵からバス鍵、すなわち一時鍵を生成する。

7bは、例えば一方性関数を利用して、2つの認証鍵からバス鍵、すなわち一時鍵を生成する。

【0059】認証鍵生成回路33aと認証鍵生成回路33bは、例えば同一のアルゴリズムを用いることにより、同一のチャレンジ鍵に対して同一の認証鍵を生成することとする。

【0060】バス鍵生成回路37aとバス鍵生成回路37bは、例えば同一のアルゴリズムを用いることにより、同一の2つの認証鍵から同一のバス鍵を生成するものとする。

【0061】次に、図2、図4を参照しながら、鍵共有手順について説明する。まず、鍵共有手順のフェイズ1では、復号化ユニット121にて、チャレンジ鍵生成回路31aによりチャレンジ鍵(Challenge Key)1を生成し、これを暗号化ユニット118にも伝える。次に、復号化ユニット121の認証鍵生成回路33aと暗号化ユニット118の認証鍵生成回路33bのそれぞれにて、チャレンジ鍵1をもとに認証鍵1(Key1)を生成し、また暗号化ユニット118から復号化ユニット121へ生成した認証鍵1を転送する。そして、復号化ユニット121にて、比較回路35aにより、復号化ユニット121と暗号化ユニット118のそれぞれで生成された2つの認証鍵1を比較する。もし一致すれば次のフェイズ2に移行する。もし一致しなければ異常終了となる。

【0062】次に、フェイズ2では、暗号化ユニット118にて、チャレンジ鍵生成回路31bによりチャレンジ鍵(Challenge Key)2を生成し、これを復号化ユニット121にも伝える。次に、暗号化ユニット118の認証鍵生成回路33bと復号化ユニット121の認証鍵生成回路33aのそれぞれにて、チャレンジ鍵2をもとに認証鍵2(Key2)を生成し、また復号化ユニット121から暗号化ユニット118へ生成した認証鍵2を転送する。そして、暗号化ユニット118にて、比較回路35bにより、暗号化ユニット118と復号化ユニット121のそれぞれで生成された2つの認証鍵2を比較する。もし一致すれば次のフェイズ3に移行する。もし一致しなければ異常終了となる。

【0063】そして、フェイズ3では、復号化ユニット121のバス鍵生成回路37aと暗号化ユニット118のバス鍵生成回路37bのそれぞれにて、認証鍵1および認証鍵2をもとにバス鍵(BUS Key)すなわち一時鍵Sk tを生成する。

【0064】これによって、復号化ユニット121と暗号化ユニット118との間で安全に一時鍵Sk tが共有化される。ステップS13では、復号化ユニット121から暗号化ユニット118へ、共有化した一時鍵Sk tを用いてデータ暗号鍵Sk1を伝える。すなわち、まず、復号化ユニット121にて、復号化回路32によりSk tでSk1を復号して、DSk t(Sk1)を得

る。次に、復号化ユニット121から暗号化ユニット118へ、DSkt (Sk1)を送る。そして、暗号化ユニット118にて、暗号化回路34により、Sk tでDSkt (Sk1)を暗号化して、Sk1を得る。

【0065】ステップS14では、暗号化ユニット118にて暗号化回路105cにより、Sk1を暗号鍵として用いて入力データDataを暗号化して、ESk1 (Data)を得る。

【0066】ステップS15では、ESk1 (Data)を記録媒体117に記録する。なお、1つの記録媒体に複数のIDが格納される場合、IDとESk1 (Data)とを対応付けて格納する。

【0067】次に、図1、図5を参照しながら、復号の際の手順について説明する。まず、記録媒体117がリムーバブルな媒体である場合には、これをディスクドライブ装置 (図示せず) にセットしておく。

【0068】ステップS21では、記録媒体117に記録されたIDを復号化ユニット121へ送る。ステップS22では、復号化ユニット121にて、送られたIDをもとに、記録領域109から、対応するSk1を検索して取り出し、復号化回路106eに与える。

【0069】ステップS23では、記録媒体117に記録されたESk1 (Data)を復号化ユニット121へ送る。ステップS24では、復号化ユニット121にて、復号化回路106eにより、Sk1を復号鍵としてESk1 (Data)を復号し、もとの入力データ (Data)を得る。

【0070】なお、復号対象となるデータの暗号化に用いた復号化ユニットと当該復号化ユニット121とが相違するものである場合、すなわち記録媒体117に暗号化データを記録したPCと当該PCが相違するものである場合、復号化ユニット121内に対応するIDとSk1の組が登録されていないので、上記のステップS22にて対応するSk1を検索して取り出すことに成功せず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体117に暗号化データを記録したPCにおいてのみ復号を行うことができる。

【0071】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図3において、ステップS12の一時鍵の共有は最初に行っても良い。また、ステップS12のIDの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録 (あるいは読み込みと暗号化と記録) を繰り返して行っても良い。

【0072】また、例えば図5において、復号化ユニッ

ト内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力 (あるいは読み込みと復号と出力) を繰り返して行っても良い。

【0073】上記の暗号化回路や復号化回路を用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号化回路の組ごとに、用いる暗号化方式を適宜決めても良い (すべて異なるようにすることも可能である)。

【0074】また、上記では暗号化回路や復号化回路は独立した回路として示したが、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において1つまたは複数のもので兼用するように構成しても構わない。すなわち、復号化ユニット121の復号化回路21と暗号化ユニット118の暗号化回路32の暗号化方式と、復号化ユニット121の復号化回路106cと暗号化ユニット118の暗号化回路105cの暗号化方式が同じである場合に、復号化ユニット121において復号化回路21と復号化回路106cを1つの回路で構成しても良いし、同様に暗号化ユニット118において暗号化回路32と暗号化回路105cを1つの回路で構成しても良い。

【0075】本実施形態では、暗号化ユニットはPC内に例えば暗号化ボードとして組み込まれCPUバスに接続されるものであったが、暗号化ユニットはディスクドライブ装置内に内蔵されることもある。

【0076】なお、図1の構成において、復号化ユニット121を2つのICチップに分離して構成することも可能である。例えば、復号化ユニット121から復号化回路106cを分離し、これに鍵共有回路30aと同じものと暗号化回路を付加してICチップ化し (これを第3ユニットとする)、復号の際には復号化ユニット121と第3ユニットとの間で鍵共有回路により一時鍵を共有化した後、復号化ユニット121から第3ユニットへCPUバス120を介して一時鍵で復号化したデータ暗号化鍵を送り、第3ユニットにてこれを一時鍵で暗号化してデータ暗号化鍵を得るようにしても良い。なお、この場合、復号化ユニット121に新たに復号化回路を付け加えても良いが、すでに存在する復号化回路を兼用しても良い。

【0077】 (第2の実施形態) 図6は、本発明の第2の実施形態に係るシステムの構成を示すブロック図である。なお、図6の鍵共有回路30a、30bの内部構成の一例を図2に示す。また、図7に本システムの暗号化の際の手順を、図4に鍵共有手順の一例を、図8に本システムの復号の際の手順をそれぞれ示す。

【0078】本実施形態は、基本的には第1の実施形態と同様の構成を有するものであり、以下では、主に相違する点について説明する。まず、暗号化ユニット118

は、図1の構成と同様であるが、復号化ユニット121から渡されたDSkt(ID)を、暗号化回路32により一時鍵で復号する点、復号されたIDを暗号化回路105cによりSk1で暗号化する点が相違する。

【0079】また、復号化ユニット121は、図1の構成に加えて、与えられたDSkt(ID)からSk1を得るための復号化回路106dとID判定回路110が付加されており、また生成したIDをも復号化回路32により一時鍵Sk1で復号化して暗号化ユニット118に送る点が相違する。

【0080】次に、図6、図7、図2、図4を参照しながら、暗号化の際の手順について説明する。ステップS31では、復号化ユニット121にて、ID生成回路108により入力データに対するIDを生成する。また、データ暗号鍵生成回路107により入力データを暗号化するための暗号鍵Sk1を生成する。そして、生成されたIDとSk1とを対応付けて復号化ユニット121内の記憶領域109に記録しておく。

【0081】ステップS32では、ステップS12と同様にして、復号化ユニット121と暗号化ユニット118との間で鍵共有手順により一時鍵Sk1を共有する。ステップS33では、復号化ユニット121から暗号化ユニット118へ、共有化した一時鍵Sk1を用いてデータ暗号鍵Sk1とIDを伝える。

【0082】すなわち、データ暗号鍵Sk1については、まず、復号化ユニット121にて、復号化回路32によりSk1でSk1を復号して、DSkt(Sk1)を得る。次に、復号化ユニット121から暗号化ユニット118へ、DSkt(Sk1)を送る。そして、暗号化ユニット118にて、暗号化回路34により、Sk1でDSkt(Sk1)を暗号化して、Sk1を得る。

【0083】また、IDについては上記と同様に、復号化ユニット121にて、復号化回路32によりSk1でIDを復号して、DSkt(ID)を得る。次に、復号化ユニット121から暗号化ユニット118へ、DSkt(ID)を送る。そして、暗号化ユニット118にて、暗号化回路34により、Sk1でDSkt(ID)を暗号化して、IDを得る。

【0084】ステップS34では、暗号化ユニット118にて、暗号化回路105cにより、Sk1を暗号鍵として用いてIDを暗号化して、ESk1(ID)を得る。そして、ESk1(ID)を記録媒体117に記録する。

【0085】ステップS35では、暗号化ユニット118にて、暗号化回路105cにより、Sk1を暗号鍵として用いて入力データDataを暗号化して、ESk1(Data)を得る。そして、ESk1(Data)を記録媒体117に記録する。

【0086】なお、1つの記録媒体に複数のESk1(ID)が格納される場合、ESk1(ID)とESk

1(Data)とを対応付けて格納する。次に、図6、図8を参照しながら、復号の際の手順について説明する。

【0087】まず、記録媒体117がリムーバブルな媒体である場合には、これをディスクドライブ装置(図示せず)に接続しておく。このドライブ装置は、記録媒体117に記録されたESk1(ID)を復号化ユニット121へ送る。

【0088】ステップS42では、復号化ユニット121にて、送られたESk1(ID)をもとに記録領域109から対応するSk1を求める。すなわち、まず、復号化回路106dにより、記録領域109に記録されている1つの暗号鍵を使って、ESk1(ID)を復号し、この結果をID候補とし、ID判定回路110に与える。また、この1つの暗号鍵に対応して記録領域109に記録されているIDをID判定回路110に与える。そして、ID判定回路110により、両者を比較して、一致しなければ、記録領域109に記憶されている他の暗号鍵を使って同様の手順を行う。そして、ID判定回路110により、両者を比較して、一致すれば、そのSk1とIDの組が求めるべきものである。記録領域109からあるいは復号化回路106からそのSk1を復号化回路106dに与える。

【0089】ステップS43では、記録媒体117に記録されたESk1(Data)を復号化ユニット121へ送る。ステップS44では、復号化ユニット121にて、復号化回路106cにより、Sk1を復号鍵としてESk1(Data)を復号し、もとの入力データを得る。

【0090】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図7において、ステップS32の一時鍵の共有は最初に行っても良い。また、ステップS31のIDの生成、Sk1の生成は、ステップS32の後に行っても良い。また、ステップS31のデータベースへの登録は、どのようなタイミングで行っても良い。また、ステップS33において、IDとSk1のいずれを先に共有しても構わない。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録(あるいは読み込みと暗号化と記録)を繰り返して行っても良い。

【0091】また、例えば図8において、復号化ユニット内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力(あるいは読み込みと復号と出力)を繰り返して行っても良い。

【0092】なお、第1の実施形態と同様に、暗号化回路や復号化回路は暗号化方式が同じであればユニット内

において1つまたは複数のもので兼用するように構成しても構わない。本実施形態では、復号化ユニット121において、復号化回路32、106c、106dを1つの回路で構成することも可能であり、また、2つの回路（例えば、復号化回路32と、復号化回路106c、106dに共用する回路）で構成することも可能である。

【0093】（第3の実施形態）図9は、本発明の第3の実施形態に係るシステムの構成を示すブロック図である。図10は、本システムの暗号化の際の手順を示すフローチャートである。図11は、本システムの復号の際の手順を示すフローチャートである。

【0094】図9に示すように、本実施形態に係るシステムは、暗号化ユニット118と復号化ユニット121を備えている。また、暗号化ユニット118と復号化ユニット121は、PCのCPUバス120に接続されている。

【0095】また、CPUバス120にはディスクドライブ装置（図示せず）が接続されており、ディスクドライブ装置により記録媒体117への読み書きが行われる。図9に示すように、暗号化ユニット118は、暗号化回路105a～105c、鍵判定回路210を備えている。暗号化ユニット118は、独立した1つのICチップとして形成されるものとする。

【0096】復号化ユニット121は、データ暗号鍵生成回路107、ID生成回路108、復号化回路106a～106c、ID/鍵情報記憶回路109を備えている。復号化ユニット121は、独立した1つのICチップとして形成されるものとする。

【0097】復号化ユニット121内には、後述する複数のマスター鍵Mk s（図中102a）が登録されている（作り込まれている）。また、暗号化ユニット118内には、復号化ユニット121と同一の複数のマスター鍵Mk s（図中102b）が登録されている（作り込まれている）。

【0098】なお、万一、マスター鍵が破られたことが発覚した場合、それ以降、復号化ユニット121には、その破られたものを除いてマスター鍵が作り込まれる。ただし、暗号化ユニット118については、その破られたものを除いてマスター鍵が作り込まれても良いし、そうしなくても良い。また、破られたマスター鍵が作り込まれている復号化ユニット203は、その破られたものを除いてマスター鍵が作り込まれている新しいものに差し替えるのが望ましい。ただし、暗号化ユニット118は、破られたマスター鍵が作り込まれているものをそのまま使用しても構わない。

【0099】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該PCのCPUで実行することにより実現することができる。データDataは、暗号化して記録する対象となる入力データであり、例えばPCのI/Oポートから入力される

映像、音声、テキストなどのマルチメディア・データである。

【0100】IDは、本実施形態では、一纏まりのデータ毎（例えばタイトル毎）に与えられる識別番号である。なお、IDは、ディスク毎に与えるようにしても良いし、ファイル毎に与えるようにしても良いし、複数のファイルからなる組毎に与えるようにしても良いし、上記の一纏まりのデータをさらに細分化した部分毎（例えばチャプター毎あるいは曲毎など）に与えるようにしても良い。

【0101】Sk 1は、データの暗号化および復号に用いるデータ暗号鍵（共通鍵暗号方式における共通鍵）であり、IDと対で生成される。Mk s（ $s=1\sim n$ 、 n は2以上の整数）は、マスター鍵（共通鍵暗号方式における共通鍵）の鍵束である。マスター鍵は、例えばメーカ毎に所定個数づつが割り当てられる。この場合、マスター鍵は、メーカ間で重複のないように割り当てられる。ここでは、一例として、 $s=1, \dots, 10$ （ $s=10$ ）とする。つまり、Mk 1, Mk 2, ..., Mk 10のマスター鍵が、暗号化ユニット118、復号化ユニット121のそれぞれに作り込まれる。

【0102】前述したように、マスター鍵の鍵束は、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0103】ID生成回路108は、ID番号を生成する。ID番号は、1から順番に発番するようにしても良いが、好ましくはランダムに発番する方が良い。後者の場合、生成されるIDが全て異なるようにするために、例えばID生成回路108を乱数発生器を用いて構成する方法が考えられる。なお、重複発番する可能性のある乱数等を用いる場合には、生成したIDが既発番のものと同じであるかどうかチェックし、重複して発番されたことが分かったならば、そのIDは破棄し、別のIDを生成し直すようにすると好ましい。

【0104】データ暗号鍵生成回路107は、IDと対になるデータ暗号鍵Sk 1を生成する。一時鍵生成回路107は、例えば鍵長分の乱数発生器で構成しても良い。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0105】ID/鍵情報記憶回路109は、対になるIDとSk 1とを対応づけて記憶するためのものである。例えば、IDとSk 1をデータベース化して保管しておく。記録媒体117は、暗号化されたI/Oポートからの入力データを記録するためのものであり、例えばハードディスク、MO、FD、1回書き込み可能なCD、DVD-RAMなどを用いることが考えられる。

【0106】なお、ディスクドライブ装置内には、記録の際に変調、誤り訂正回路を行い、再生の際に復調、誤り訂正回路を行う変復調／誤り訂正回路が内蔵される場合がある。

【0107】また、本実施形態では、復号化ユニット121はデジタルデータからアナログデータに変換するD/A変換回路が備えられ、復号化ユニット121からはアナログに変換されデータが出力されるものとする。また、デジタルデータDataが復号すべきものである場合にはこれを復号する復号回路をD/A変換回路の前に設けるものとする。例えばデジタルデータDataがMPEG方式で圧縮された画像データである場合に、MPEG復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット121からの出力は例えば画像としてディスプレイなどに表示される。

【0108】最初に、図9、図10を参照しながら、暗号化の際の手順について説明する。まず、記録媒体117がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【0109】ステップS51では、復号化ユニット121にて、ID生成回路108により入力データに対するIDを生成する。また、データ暗号鍵生成回路107により入力データを暗号化するための暗号鍵Sk1を生成する。そして、生成されたIDとSk1とを対応付けて復号化ユニット121内の記憶領域109に記録しておく。また、生成されたIDを記録媒体117に記録する。

【0110】なお、IDは、復号化ユニット121からCPUバスを介して直接、ディスクドライブ装置に与えても良いし、復号化ユニット121からCPUバスを介して暗号化ユニット118に与え、暗号化ユニット118からCPUバスを介してディスクドライブ装置に与えるようにしても良い。

【0111】ステップS52では、以下に示すような手順を用いて、復号化ユニット121から暗号化ユニット118へ、生成されたデータ暗号鍵Sk1を伝える。Sk1のブレインデータを取得されないように、Sk1は、復号化ユニット121内に記録されたマスター鍵Mks ($s=1, \dots, n$) のうちのいずれか（これをMkiとする）で暗号化され、EMki (Sk1) としてCPUバス120を通過して暗号化ユニット118へ送られる。

【0112】ここで、もしマスター鍵が1つだけ存在するのであれば（これをMk0とする）、単に復号化ユニット121にてMk0でSk1を復号し、このEMk0 (Sk1) を暗号化ユニット118へ送り、暗号化ユニ

ット118にてMk0でEMk0 (Sk1) を暗号化することにより、Sk1を取り出すことができるが、本実施形態では、複数のマスター鍵からなる鍵束のうちの使用したマスター鍵Mkiを直接的に指し示す識別情報は復号化ユニット121から暗号化ユニット118へ伝えない。ようにし、代わりに、上記マスター鍵Mkiを特定可能とする情報を復号化ユニット121から復号化ユニット121へ送り、暗号化ユニット118にて、Sk1の復号に使用されたマスター鍵Mkiがn個のマスター鍵のうちのいずれであるかを特定するとともに、このマスター鍵の特定を通じてSk1を得る。

【0113】以下、ステップS52のより詳しい手順について説明する。まず、復号化ユニット121にて、復号化回路106aにより、n個のマスター鍵Mks ($i=1, \dots, n$) のうちから例えばランダムあるいは順番に選んだ1つ（これをMkiとする）でデータ暗号化鍵Sk1を復号して、DMki (Sk1) を得る。また、復号化回路106bにより、Sk1自身を復号鍵として用いてSk1を復号して、DSk1 (Sk1) を得る。そして、DMki (Sk1) とDSk1 (Sk1) を、CPUバス120を通じて暗号化ユニット118へ送る。

【0114】次に、暗号化ユニット118にて、まずマスター鍵を1つ選ぶ（これをMkpとする）。選んだMkpを復号鍵として、暗号化回路105aにより、DMki (Sk1) を暗号化し、 $EMkp (DMki (Sk1)) = Ska$ を得る。

【0115】次に、暗号化回路105aの出力Skaを復号鍵として、暗号化回路105bにより、DSk1 (Sk1) を暗号化し、 $ESka (DSk1 (Sk1)) = Skb$ を得る。

【0116】次に、鍵判定回路210により、SkaとSkbとが一致するか否か調べる。ここで、復号化ユニット121にてSk1を暗号化したマスター鍵MkiがMkpであったならば、 $Ska = EMkp (DMki (Sk1)) = Sk1$ となり、従って、 $Skb = ESka (DSk1 (Sk1)) = ESkl (DSkl (Sk1)) = Sk1$ となり、ゆえに、 $Ska = Skb = Sk1$ となる。

【0117】つまり、鍵判定回路210により、SkaとSkbとが一致することがわかった場合には、Mki = Mkp、かつ、 $Ska = Skb = Sk1$ であり、この場合、鍵判定回路210は $Ska = Skb = Sk1$ を出力する。

【0118】一方、鍵判定回路210により、Skaと

S k b とが一致しないことがわかった場合には、M k i ≠ M k p であり、復号化ユニット 1 2 1 にて S k 1 はこの M k p では暗号化されておらず、それ以外のマスター鍵で暗号化されたことが判る。この場合、鍵判定回路 2 1 0 は出力をしない（あるいは鍵判定回路 2 1 0 の出力が暗号化回路 1 0 5 a には伝達されない）。

【0 1 1 9】以降は、S k a と S k b とが一致するまで、暗号化に用いるマスター鍵 M k p を変更して、上記の手順を繰り返す。例えば、最初に M k p として M k 1 を用いて上記の手順を行って S k a と S k b とが一致しなかつた場合に、次に M k 2 へと更新して再び上記の手順を繰り返すのである。

【0 1 2 0】以上のような手順を用いて、復号化ユニット 1 2 1 にてどのマスター鍵を用いたのかを暗号化ユニット 1 1 8 側で特定することができるとともに、復号化ユニット 1 2 1 と暗号化ユニット 1 1 8 との間でデータ暗号化鍵 S k 1 を安全に共有することが可能となる。

【0 1 2 1】ステップ S 5 3 では、暗号化ユニット 1 1 8 にて、暗号化回路 1 0 5 c により、S k 1 を暗号鍵として用いて入力データ D a t a を暗号化して、E S k 1 (D a t a) を得る。

【0 1 2 2】ステップ S 5 4 では、E S k 1 (D a t a) を記録媒体 1 1 7 に記録する。なお、1 つの記録媒体に複数の I D が格納される場合、I D と E S k 1 (D a t a) とを対応付けて格納する。

【0 1 2 3】次に、図 9、図 1 1 を参照しながら、復号の際の手順について説明する。まず、記録媒体 1 1 7 がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【0 1 2 4】ステップ S 6 1 では、記録媒体 1 1 7 に記録された I D を復号化ユニット 1 2 1 へ送る。ステップ S 6 2 では、復号化ユニット 1 2 1 にて、送られた I D をもとに、記録領域 1 0 9 から、対応する S k 1 を検索して取り出し、復号化回路 1 0 6 e に与える。

【0 1 2 5】ステップ S 6 3 では、記録媒体 1 1 7 に記録された E S k 1 (D a t a) を復号化ユニット 1 2 1 へ送る。ステップ S 6 4 では、復号化ユニット 1 2 1 にて、復号化回路 1 0 6 e により、S k 1 を復号鍵として E S k 1 (D a t a) を復号し、もとの入力データ (D a t a) を得る。

【0 1 2 6】なお、復号対象となるデータの暗号化に用いた復号化ユニットと当該復号化ユニット 1 2 1 とが相違するものである場合、すなわち記録媒体 1 1 7 に暗号化データを記録した P C と当該 P C が相違するものである場合、復号化ユニット 1 2 1 内に対応する I D と S k 1 の組が登録されていないので、上記のステップ S 2 2 にて対応する S k 1 を検索して取り出すことに成功せず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体 1 1 7 に暗号化データを記録した P C においてのみ復号を行

うことができる。

【0 1 2 7】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図 1 0 において、ステップ S 5 1 の I D の生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行ってもよい。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでもよい。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録（あるいは読み込みと暗号化と記録）を繰り返し行ってもよい。図 1 1 については、第 1 の実施形態と同様である。

【0 1 2 8】上記の暗号化回路や復号化回路で用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号化回路の組ごとに、用いる暗号化方式を適宜決めても良い（すべて異なるようにすることも可能である）。

【0 1 2 9】また、上記では暗号化回路や復号化回路は独立した回路として示したが、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において 1 つまたは複数のもので兼用するように構成しても構わない。例えば、復号化ユニット 1 2 1 において、復号化回路 1 0 6 a, 1 0 6 b, 1 0 6 c を 1 つの回路で構成することも可能であり、また、2 つの回路（例えば、復号化回路 1 0 6 a, 1 0 6 b に共用する回路と、復号化回路 1 0 6 c）で構成することも可能である。また、例えば、暗号化ユニット 1 1 8 において、暗号化回路 1 0 5 a, 1 0 5 b, 1 0 5 c を 1 つの回路で構成することも可能であり、また、2 つの回路（例えば、暗号化回路 1 0 5 a, 1 0 5 b に共用する回路と、暗号化回路 1 0 5 c）で構成することも可能である。

【0 1 3 0】なお、第 1 の実施形態と同様に、図 9 の構成においても、復号化ユニット 1 2 1 を 2 つの I C チップに分離して構成することも可能である。

（第 4 の実施形態）図 1 2 は、本発明の第 4 の実施形態に係るシステムの構成を示すブロック図である。図 1 3 は、本システムの暗号化の際の手順を示すフローチャートである。図 1 4 は、本システムの復号の際の手順を示すフローチャートである。

【0 1 3 1】本実施形態は、基本的には第 3 の実施形態と同様の構成を有するものであり、以下では、主に相違する点について説明する。まず、暗号化ユニット 1 1 8 は、図 9 の構成と同様であるが、復号化ユニット 1 2 1 から渡された D M k i (I D) を、マスター鍵 M k i が特定された後に暗号化回路 1 0 5 a によりこのマスター鍵 M k i で復号する点、復号された I D を暗号化回路 1 0 5 c により S k 1 で暗号化する点が相違する。

【0 1 3 2】また、復号化ユニット 1 2 1 は、図 9 の構成に加えて、与えられた E S k 1 (I D) から S k 1 を得るための復号化回路 1 0 6 d と I D 判定回路 1 1 0 が付加されており、また生成した I D をも復号化回路 1 0

6aによりマスター鍵Mk_iで復号化して暗号化ユニット118に送る点が相違している。

【0133】次に、図12、図13を参照しながら、暗号化の際の手順について説明する。ステップS71では、復号化ユニット121にて、ID生成回路108にトリガデータを入力してIDを生成する。また、データ暗号鍵生成回路107により入力データを暗号化するための暗号鍵Sk₁を生成する。そして、生成されたIDとSk₁とを対応付けて復号化ユニット121内の記憶領域109に記録しておく。

【0134】ステップS72では、以下に示すような手順を用いて、復号化ユニット121から暗号化ユニット118へ、生成されたデータ暗号鍵Sk₁とIDを伝える。まず、復号化ユニット121にて、復号化回路106aにより、n個のマスター鍵Mk_s (s=1, ..., n) のうちのいずれか (これをMk_iとする) でデータ暗号化鍵Sk₁を復号して、DMk_i (Sk₁) を得る。また、復号化回路106bにより、Sk₁自身を復号鍵として用いてSk₁を復号して、DSk₁ (Sk₁) を得る。そして、DMk_i (Sk₁) とDSk₁ (Sk₁) を、CPUバス120を通じて暗号化ユニット118へ送る。また、復号化回路106aにより、IDも同じMk_iで復号して、DMk_i (ID) を求め、これもCPUバス120を通じて暗号化ユニット118へ送る。

【0135】次に、ステップS52と同様にして、暗号化ユニット118にて、マスター鍵Mk_iを特定するとともに、データ暗号化鍵Sk₁を求める。そして、暗号化回路105aにより、特定したMk_iでEMk_i (ID) を復号して、IDを得る。

【0136】ステップS73では、暗号化ユニット118にて、暗号化回路105cにより、Sk₁を暗号鍵として用いてIDを暗号化して、ESk₁ (ID) を得る。そして、ESk₁ (ID) を記録媒体117に記録する。

【0137】ステップS74では、暗号化ユニット118にて、暗号化回路105cにより、Sk₁を暗号鍵として用いて入力データDataを暗号化して、ESk₁ (Data) を得る。そして、ESk₁ (Data) を記録媒体117に記録する。

【0138】なお、1つの記録媒体に複数のESk₁ (ID) が格納される場合、ESk₁ (ID) とESk₁ (Data) とを対応付けて格納する。次に、図12、図14を参照しながら、復号の際の手順について説明する。

【0139】まず、記録媒体117がリムーバブルな媒体である場合には、これをディスクドライブ装置 (図示せず) にセットしておく。ステップS81では、記録媒体117に記録されたESk₁ (ID) を復号化ユニット121へ送る。

【0140】ステップS82では、復号化ユニット121にて、送られたESk₁ (ID) をもとに記録領域109から対応するSk₁を求める。すなわち、まず、復号化回路106dにより、記録領域109に記録されている1つの暗号鍵を使って、ESk₁ (ID) を復号し、この結果をID候補とし、ID判定回路110に与える。また、この1つの暗号鍵に対応して記録領域109に記録されているIDをID判定回路110に与える。そして、ID判定回路110により、両者を比較して、一致しなければ、記録領域109に記憶されている他の暗号鍵を使って同様の手順を行う。そして、ID判定回路110により、両者を比較して、一致すれば、そのSk₁とIDの組が求めるべきものであるので、記録領域109からあるいは復号化回路106からそのSk₁を復号化回路106dに与える。

【0141】ステップS83では、記録媒体117に記録されたESk₁ (Data) を復号化ユニット121へ送る。ステップS84では、復号化ユニット121にて、復号化回路106cにより、Sk₁を復号鍵としてESk₁ (Data) を復号し、もとの入力データを得る。

【0142】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図13において、ステップS71のIDの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録 (あるいは読み込みと暗号化と記録) を繰り返し行っても良い。図11については、第2の実施形態と同様である。

【0143】第3の実施形態と同様に、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において1つまたは複数のもので兼用するように構成しても構わない。本実施形態では、例えば、復号化ユニット121において、復号化回路106a、106b、106c、106dを1つの回路で構成することも可能であり、また、2つの回路 (例えば、復号化回路106a、106bに共用する回路と、復号化回路106c、106dに共用する回路) で構成することも可能であり、また、3つの回路で構成することも可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0144】

【発明の効果】本発明によれば、その都度生成するデータ暗号化鍵を識別情報と対応させてユニット内に記録しておくことにより、このユニットそのものがなければ復号を行うことができず、記録媒体の複製を作っても他の計算機では復号することができない。

【0145】また、本発明によれば、CPUバスを流れるデータ暗号化鍵は暗号化されており、またデータ暗号化鍵自体もその都度生成されるものであるため、第3者により暗号を解読することは極めて困難である。したがって、本発明によれば、第3者による不正なコピーを防止することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るシステムの構成を示すブロック図

【図2】図1の鍵共有回路の内部構成の一例を示す図 10

【図3】同実施形態における暗号化の際の手順を示すフローチャート

【図4】鍵共有手順の一例を示すフローチャート

【図5】同実施形態における復号の際の手順を示すフローチャート

【図6】本発明の第2の実施形態に係るシステムの構成を示すブロック図

【図7】同実施形態における暗号化の際の手順を示すフローチャート

【図8】同実施形態における復号の際の手順を示すフローチャート 20

【図9】本発明の第3の実施形態に係るシステムの構成を示すブロック図

【図10】同実施形態における暗号化の際の手順を示すフローチャート

【図11】同実施形態における復号の際の手順を示すフ

ローチャート

【図12】本発明の第4の実施形態に係るシステムの構成を示すブロック図

【図13】同実施形態における暗号化の際の手順を示すフローチャート

【図14】同実施形態における復号の際の手順を示すフローチャート

【符号の説明】

30 a, 30 b…鍵共有回路

31 a, 31 b…チャレンジ鍵生成回路

33 a, 33 b…認証鍵生成回路

35 a, 35 b…比較回路

37 a, 37 b…バス鍵生成回路

102 a, 102 b…マスター鍵の鍵束

105 a～105 c…暗号化回路

106 a～106 d…復号化回路

107…データ暗号鍵生成回路

108…ID生成回路

109…ID/鍵情報記憶回路

110…ID判定回路

117…記録媒体

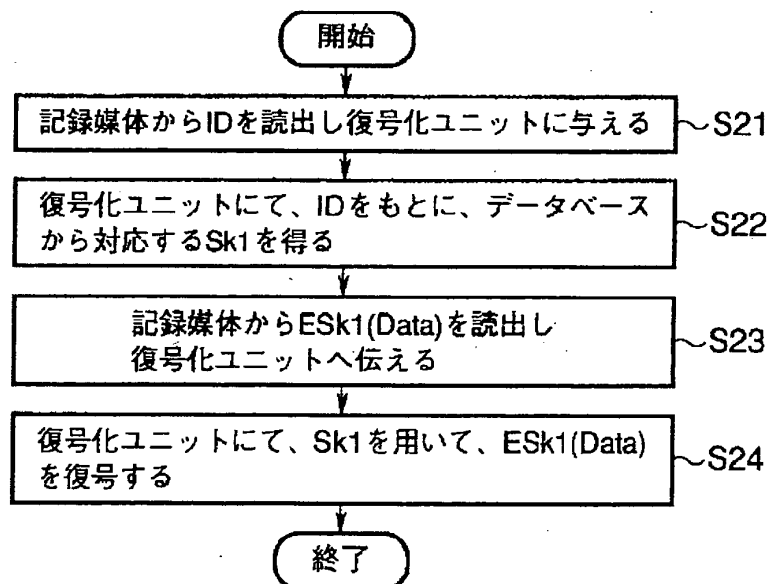
118…暗号化ユニット

120…CPUバス

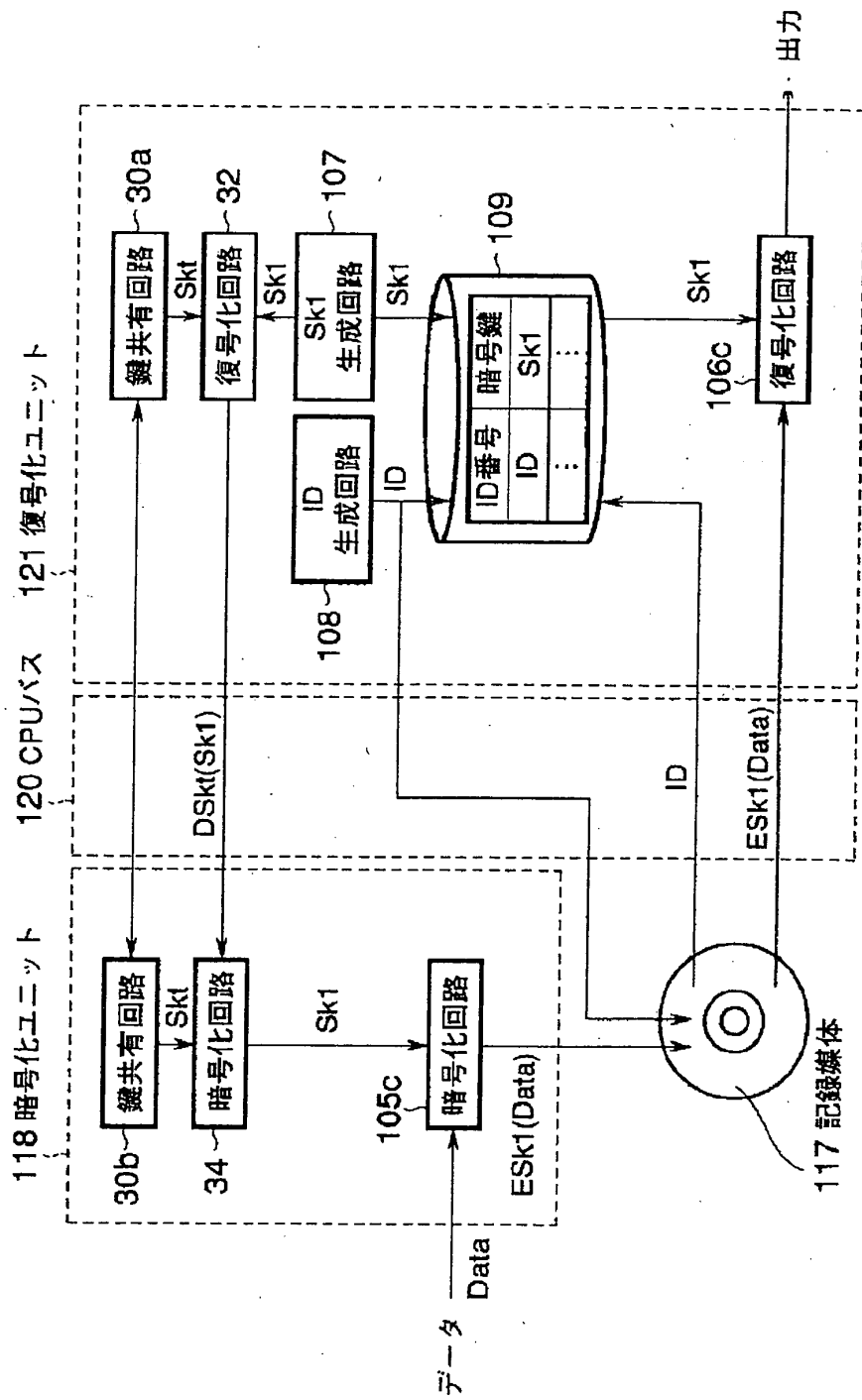
121…復号化ユニット

210…鍵判定回路

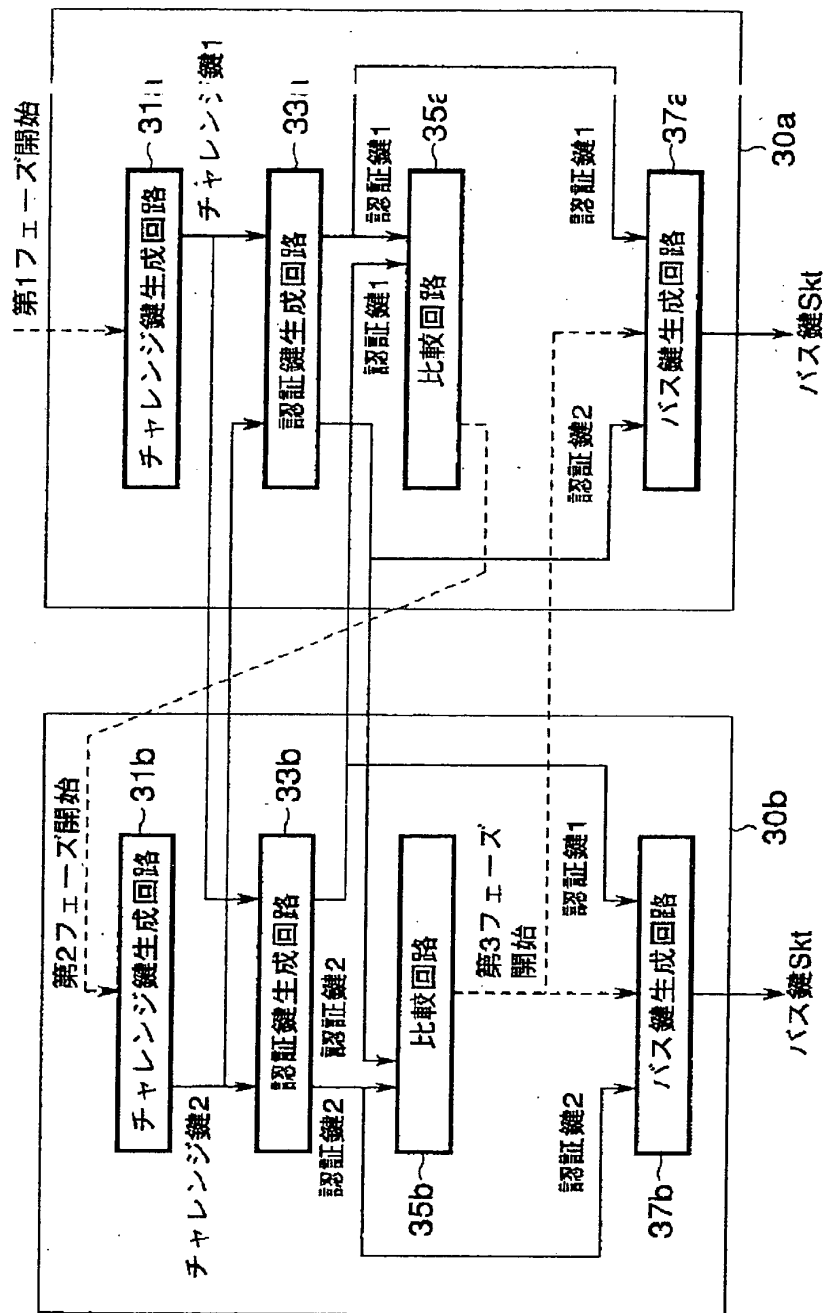
【図5】



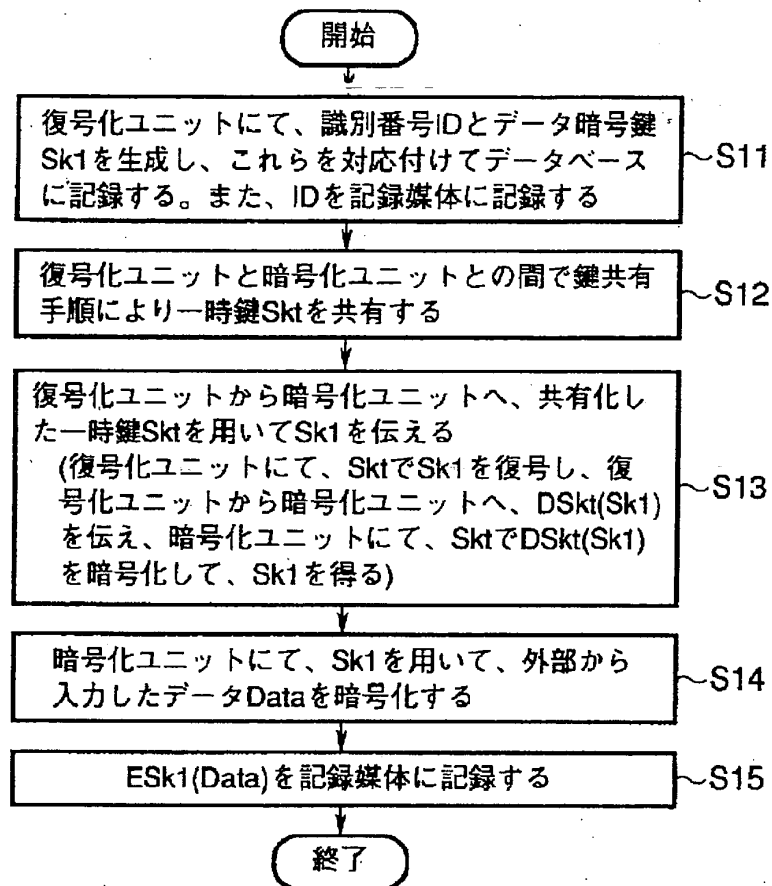
【図1】



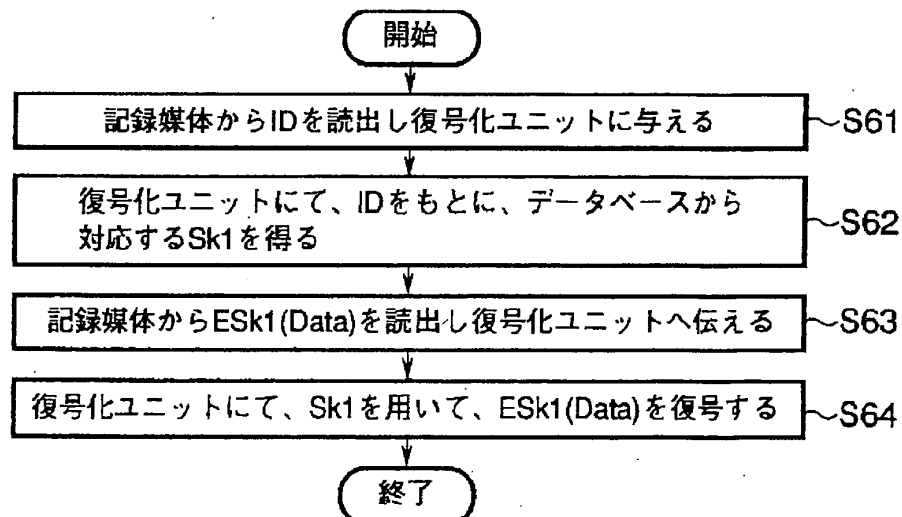
【図2】



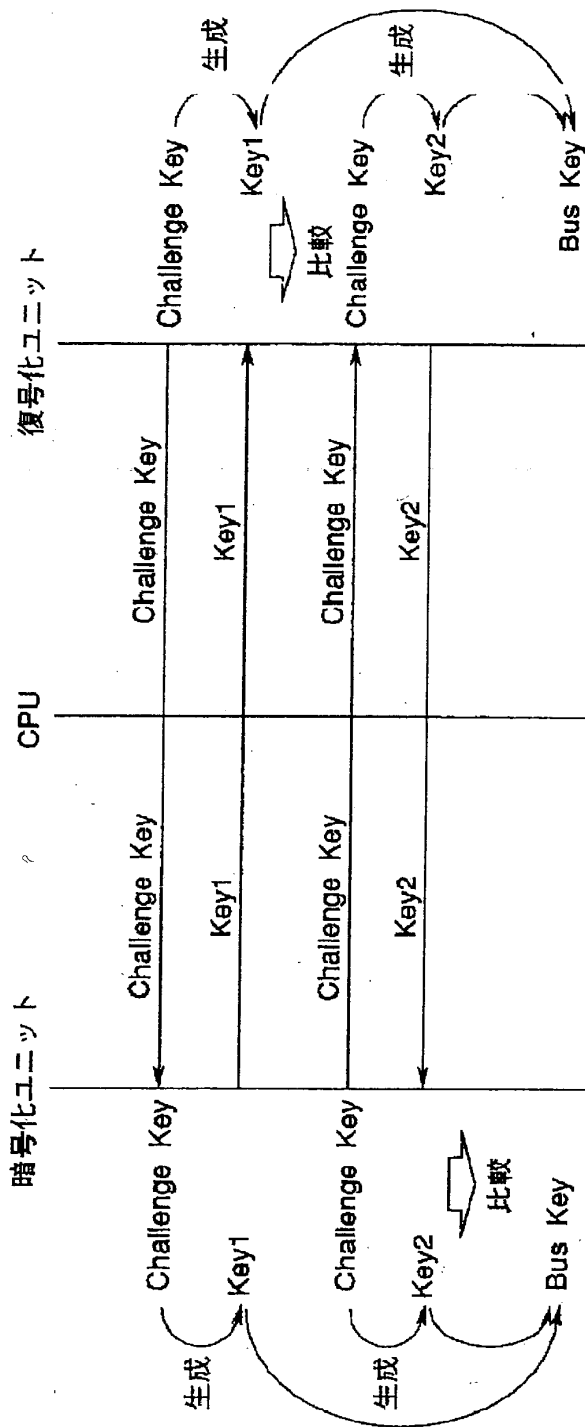
【図3】



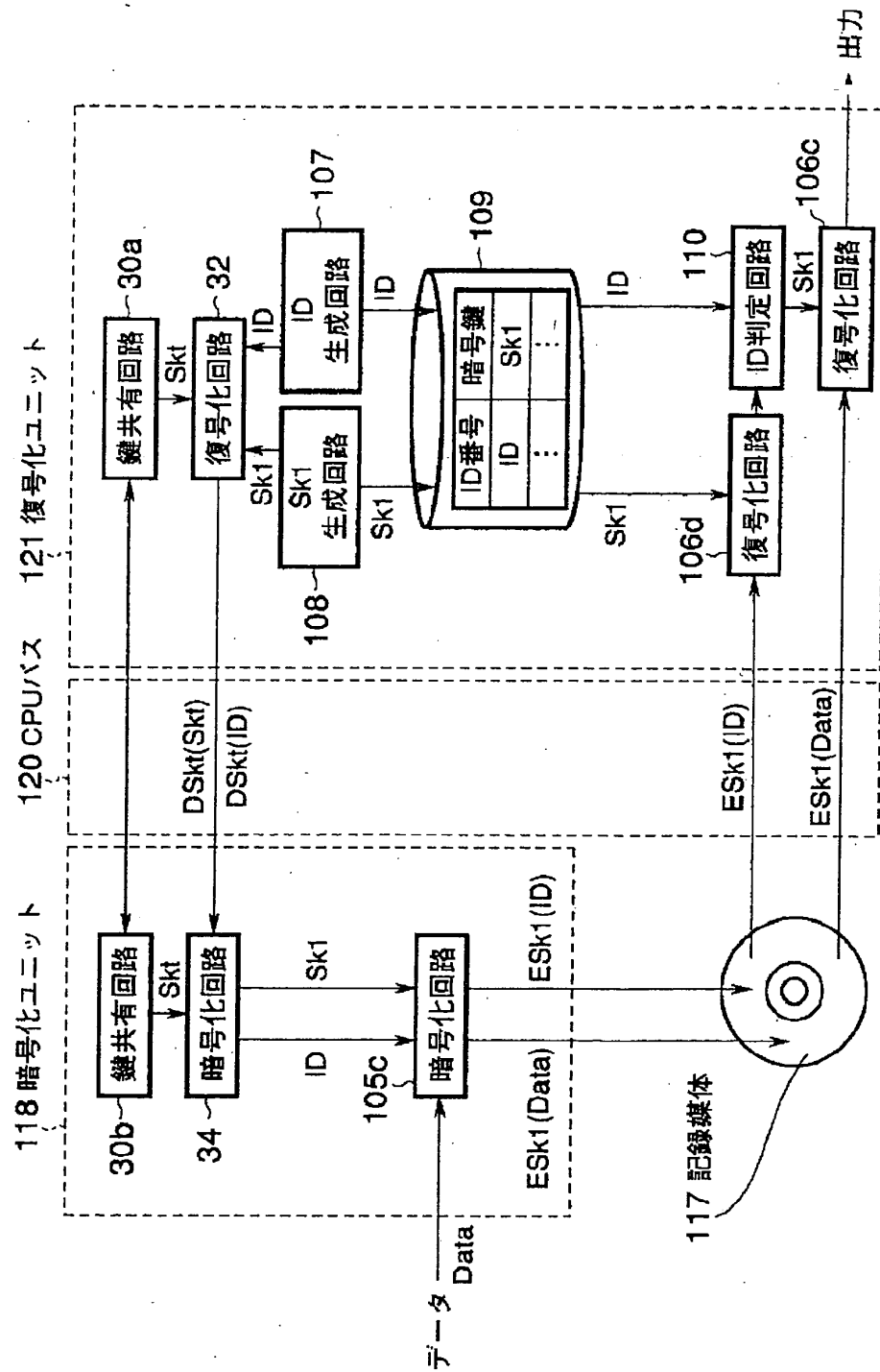
【図11】



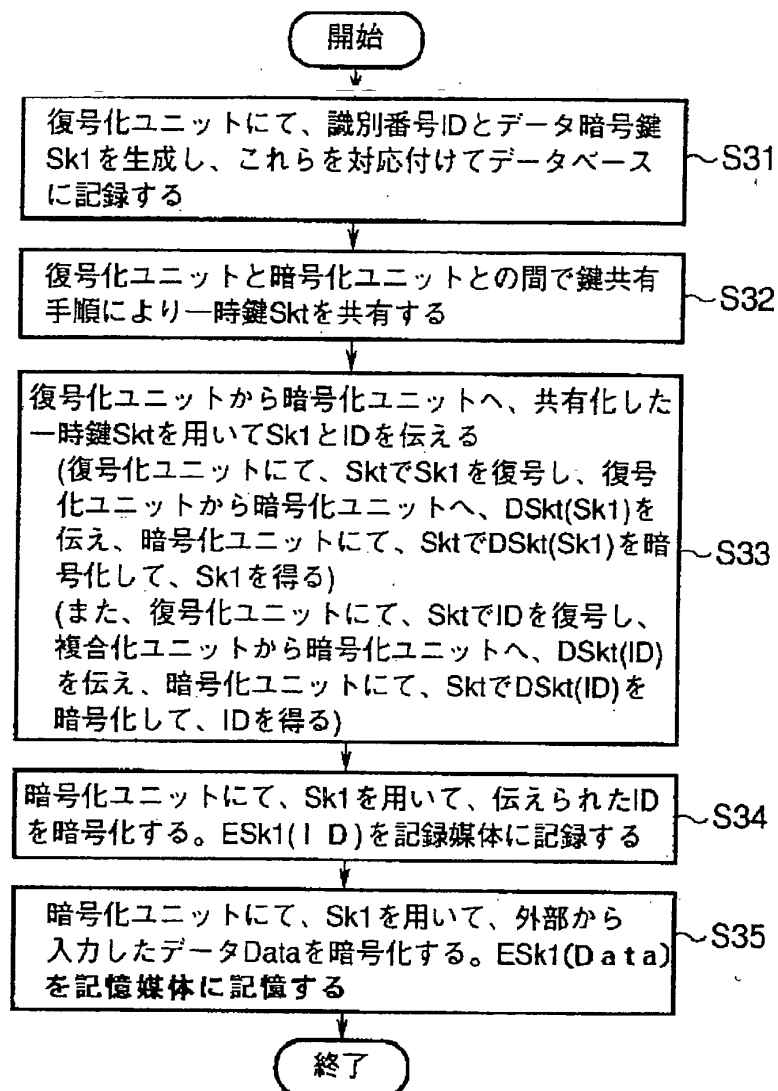
【図4】



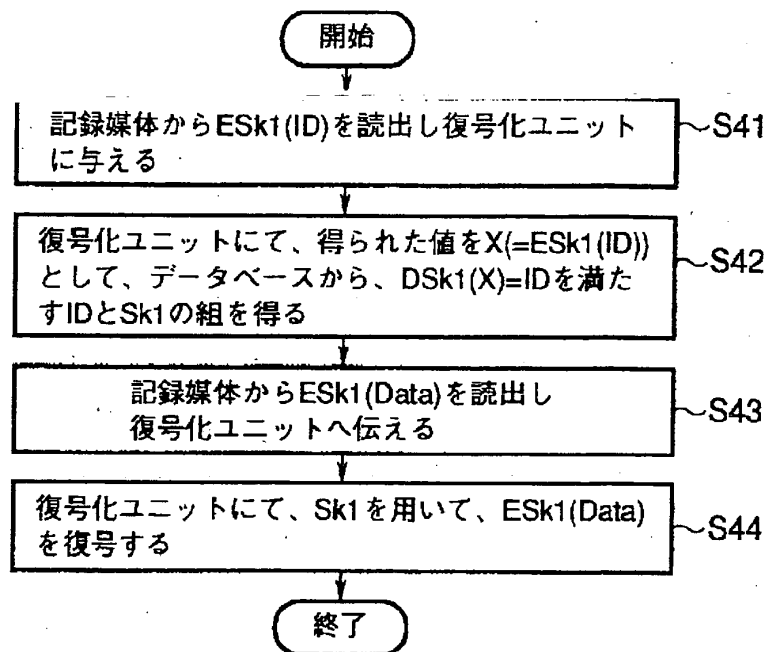
【図6】



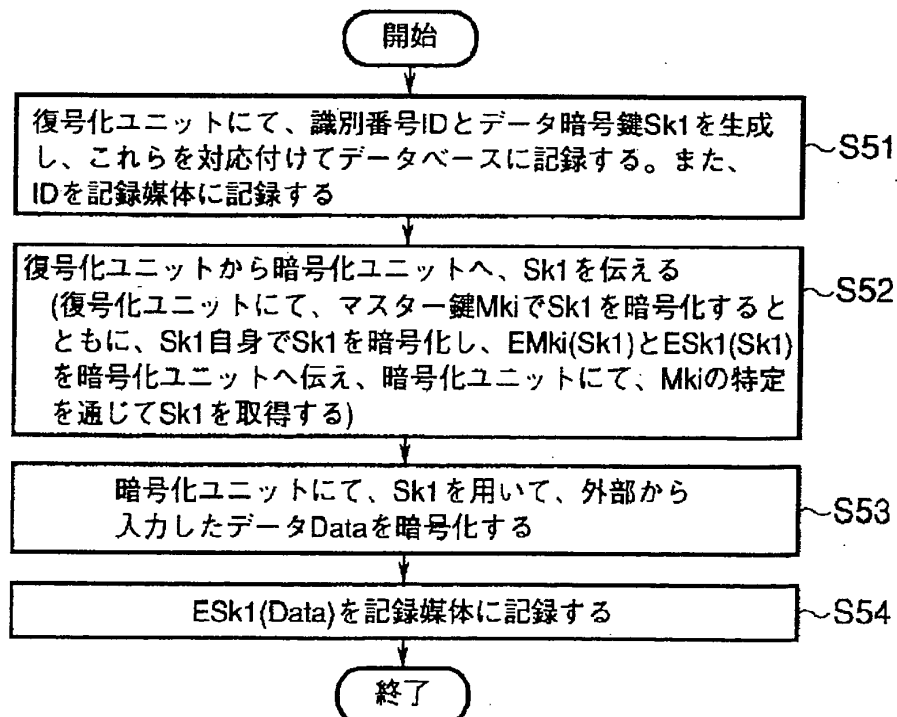
【図7】



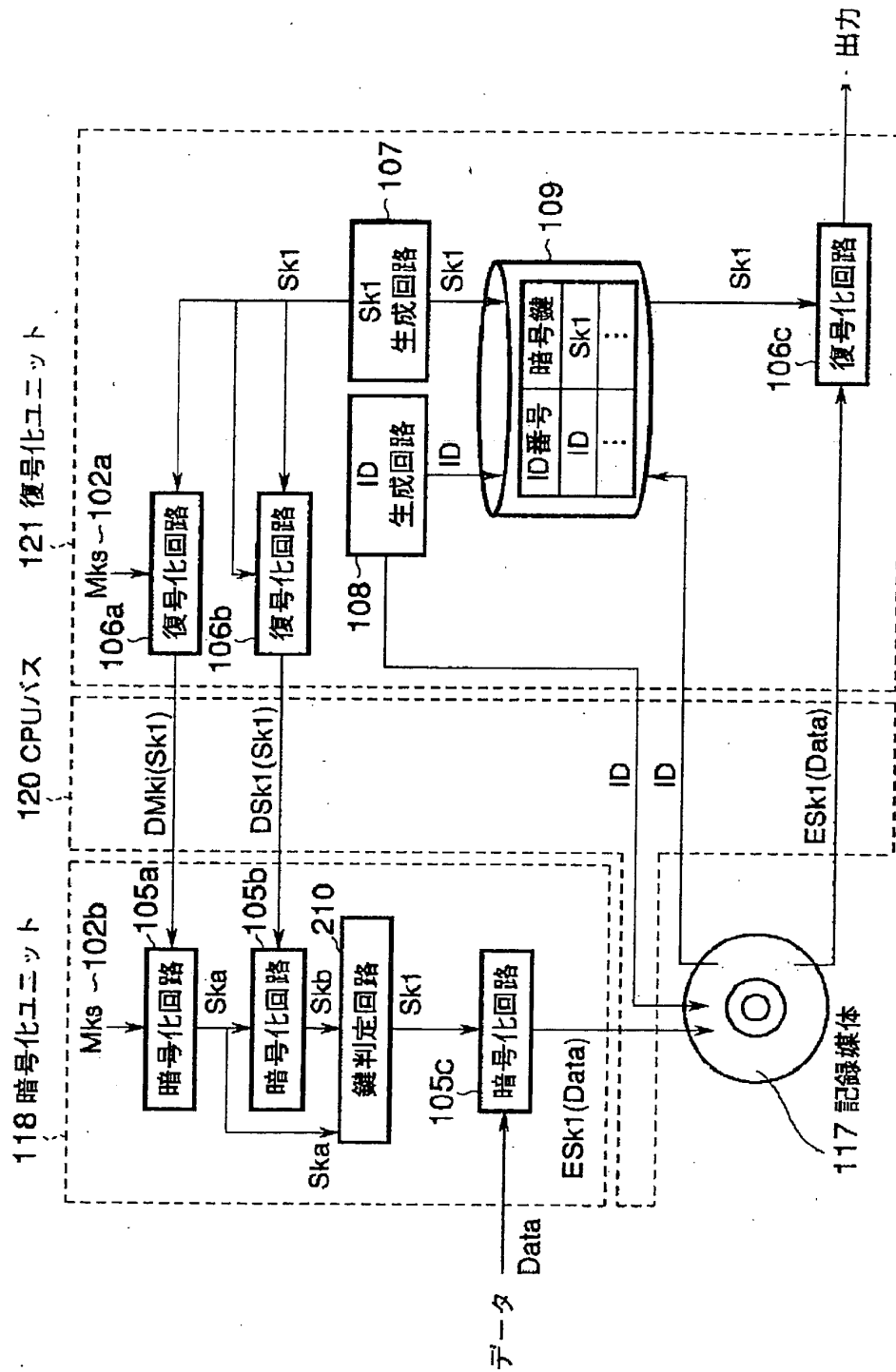
【図8】



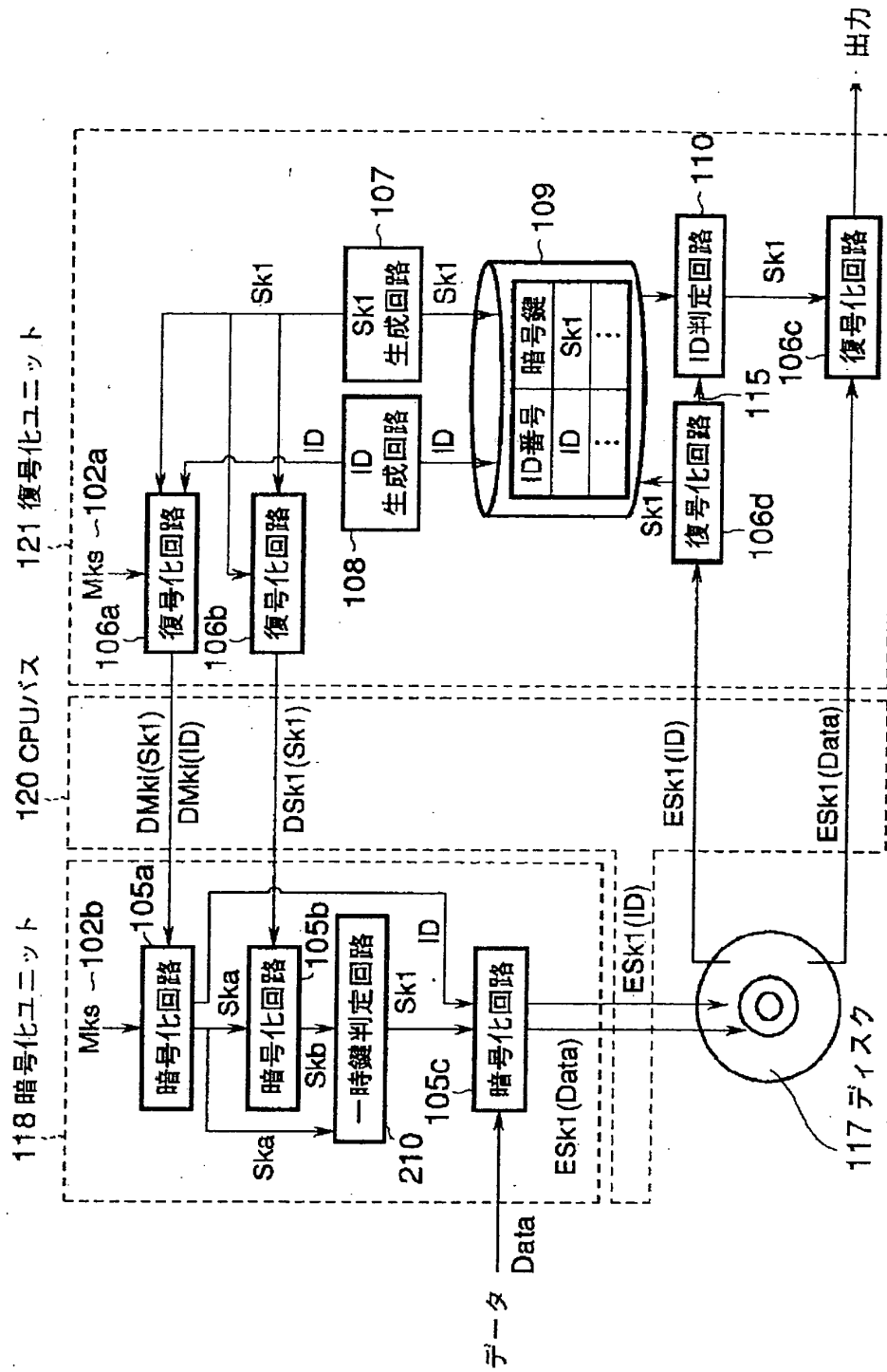
【図10】



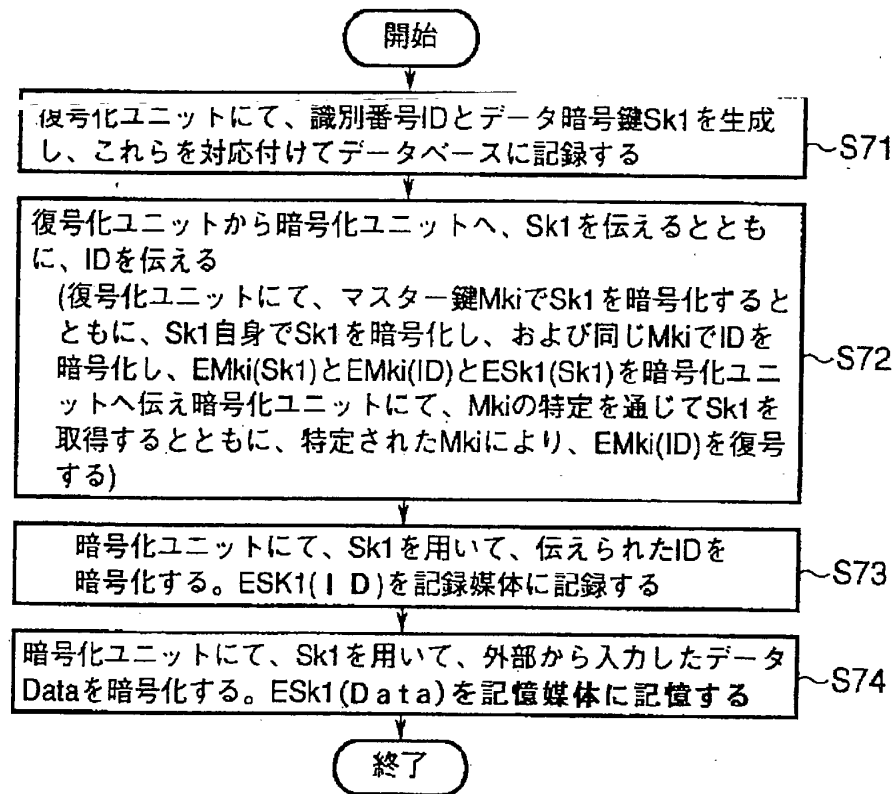
【図9】



【図12】



【図13】



【図14】

